



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/786,072

02/26/2004

Yohsuke Ishii

MEI-101

3877

24956

7590

10/23/2006

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 DIAGONAL ROAD  
SUITE 370  
ALEXANDRIA, VA 22314

EXAMINER

DARNO, PATRICK A

ART UNIT

PAPER NUMBER

2163

DATE MAILED: 10/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 10/786,072	<b>Applicant(s)</b> ISHII ET AL.	
	<b>Examiner</b> Patrick A. Darno	<b>Art Unit</b> 2163	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 25 July 2006.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-5, 8-11, 14-28 are as previously presented. Claims 6-7 and 12-13 are in their original form. Claims 1-28 are pending in this Office Action.

#### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-2, 4, 15-17, 19, 21-22, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication Number 2004/0254934 issued to Mang-Rong Ho et al. (hereinafter "Ho") in view of U.S. Patent Application Publication issued to Jude Jacob Kavalam et al. (hereinafter "Kavalam") and further in view of U.S. Patent Number 5,260,551 issued to Tore Wiik et al. (hereinafter "Wiik").

#### **Claims 1, 15, 19, 21, 22, 24:**

The combination of Ho, Kavalam, and Wiik discloses an access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

and Ho explicitly discloses the access controller comprising:

an access restriction module (*Ho: paragraph [0004], lines 1-9 and paragraph [0009], lines 7-9 and paragraph [0010], lines 7-9; The content management system is the access restriction module.*) configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded (*Ho: paragraph [0003], lines 2-9 and paragraphs [0028]-[0031] and paragraph [0078], lines 6-10; Note specifically in the first reference cited "storage of an access control list (ACL) for each data entity to which access is to be controlled." Paragraph [0001], lines 9-11 defines a data entity.*).

Ho does not explicitly disclose:

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition list of the access controller;

an input module configured to input user information corresponding to the access prohibited user; and

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or the updated access prohibition list to the other access controllers in response to the update

a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of each access controller connected with the network, according to the received user information input through the input module or the updated access prohibited list.

Kavalam also discloses an access control module to control access to network resources with the use of access control lists (*Kavalam: Fig. 1, 116 and paragraph [0062], lines 5-8*). Examiner notes that Kavalam does not explicitly disclose the use of an access prohibition list (or black-list)

Art Unit: 2163

to intercept or restrict user access, but Kavalam does explicitly suggest protecting system resources by such strategies “lock down”, isolation, and sandboxing of users or systems when either accidental or malicious actions occur that could harm system resources (*Kavalam: paragraph [23], lines 23-28*). In order to “lock down”, isolate, or sandbox a particular user or system, a system administrator would have to have some means to detect that an accidental or malicious act either has already occurred, is currently occurring, or may occur in the future.

In order to satisfy the suggestion of combining additional methods of protecting system resources with the use of an access control module using access control lists, examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ho, as suggested by Kavalam with the teachings of Wiik noted below.

Wiik explicitly discloses:

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition listed on an access prohibition list on an access prohibition list of the access controller (*Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.*);

an input module configured to input user information corresponding to the access prohibited user (*Wiik: column 5, lines 9-11; The lock communicator (admin access controller) is used to update*

Art Unit: 2163

*the black-list (or prohibited user list). The list has a capacity of 20 users. There must be some form of input module to add a user to the black-list.);*

at least one of the access controllers having the updated access prohibition list further comprising a distribution module configured to send out the user information or the updated access prohibition list to the to the other access controllers in response to the update (*Wiik: column 5, 7-11 and column 5, lines 56-63 and column 4, lines 32-38; The "lock communicator" (or admin access controller) oversees each individual locking mechanism (or access interception module or access controller). Since the lock communicator controls the access controller (locking mechanism), the lock communicator itself is also an access controller. From the cited references it can be see that the lock communicator (access controller) downloads (updates) new user information (user ID) to the black-list. The transfer of this information from the lock communicator to the locking mechanism must be done through a distribution module.); and,*

a list update module configured to receive the user information or the updated access prohibition list and to update the access prohibition list of each access controller connected with the network, according to the received user information input through the input module or the updated access prohibited list (*Wiik: column 5, lines 9-11; The black-list is updated by the lock communicator (or admin access controller) according to user ID's. Note that the update to the black list is received at the access controller (locking mechanism). There must be some form of receiving module to receive the update. Further note that the update to the black-list can be an addition ("lock communicator is used to fill the list with black listed ID's") or deletions ("lock communicator also has an un-black-list function").).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a black-list, or prohibited user list, as part of an access controller (*Wiik: column 5, lines 7-11*). The skilled artisan would have been motivated to improve the invention of

Art Unit: 2163

Ho per the above such that upon making a decision to cancel a given individual's access rights, the individual could be added to a black-list resulting in the immediate loss of access to a given resource (*Wiik: column 5, lines 7-11 and column 8, lines 11-14*).

**Claim 2, 16, 17 and 25:**

The combination of Ho, Kavalam, and Wiik discloses all the elements of claims 1 and 24, as noted above, and Wiik further discloses wherein the list update module sends out to the other access controllers a registration instruction to register the input user information on the access prohibition list of the other access controllers (*Wiik: column 4, lines 35-38 and column 5, lines 7-11; Note the lock communicator (admin access controller) sends out newly added user ID's to the black-list (prohibited list) which is stored in the RAM of individual access controllers (locking mechanisms). This updates the black-list. Further note that lock communicator (admin access controller) is used to configure all locking mechanisms (access controllers) (Wiik: column 5, lines 56-59).*).

**Claim 4:**

The combination of Ho, Kavalam, and Wiik discloses all the elements of claim 1, as noted above, and Wiik further discloses wherein the access interception module also intercepts an access that has not been completed (*Wiik: column 8, lines 11-15; When the access is denied (by not unlocking the locking mechanism or access controller due to inclusion on a black-list), the access is interrupted and therefore not completed.*).

3. Claims 3 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam, in view of Wiik, and further in view of U.S. Patent Application Publication Number 2003/0018747 issued to Bjarne Geir Herland et al. (hereinafter "Herland").

**Claims 3 and 26:**

The combination of Ho, Kavalam, and Wiik discloses all the elements of claims 1 and 24, as noted above, but does not explicitly disclose wherein the list update module sends out an updated access prohibition list to the other access controllers.

However, it is important to note that Wiik does explicitly suggest the sending of at least one user from a main access controller (administrator or lock communicator) to a specific access controller (locking mechanism) (*Wiik: column 5, lines 7-11 and column 4, lines 35-38*). While the Wiik reference doesn't explicitly state sending an entire black-list, as noted above, it certainly does not eliminate the possibility of sending the entire list, and as noted above, the Wiik reference suggests the sending of at least one user to a remote access controller (locking mechanism).

Furthermore, Herland discloses wherein the list update module sends out an updated access prohibition list to the other access controllers (*Herland: paragraph [0034], lines 5-6; The examiner maintains that all that is being claimed by the applicant, in claim 3, is at most, simply sending an updated list to multiple destinations over a network. This is clearly shown in the Herland reference with the phrase "send an updated list of users to each user on the web page at that time." There is no evidence in the applicant's disclosure, the Herland reference, or recited in the applicant's arguments that lead the examiner to believe that the sending of a list as shown by Herland is patentably distinct from the way the applicant sends a list. Therefore the examiner maintains this rejection.*).

It would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the teachings of the previously mentioned combination noted above for the purpose of sending an updated list of users (*Herland: paragraph [0034], lines 5-6*). The skilled artisan would have been motivated to improve the previously mentioned combination per the above



Art Unit: 2163

such that an updated list of users could be sent across a network to update a second list of users at a remote location for the purpose of keeping a list of all users logged in to a virtual location (website) (*Herland*: paragraph [0010], lines 1-3 and paragraph [0033] and paragraph [0034], lines 1-6; *The examiner would like to bring to the applicant's attention that the reason or motivation to modify the reference may often suggest what the inventor has done, but for a different purpose or to solve a different problem. It is not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by the applicant (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)).*

4. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view Kavalam in view of Wiik and further in view of U.S. Patent Application Publication Number 2003/0041088 issued to Marc D. Wilson et al. (hereinafter "Wilson").

**Claim 5:**

The combination Ho, Kavalam, and Wiik discloses all the elements of claim 1, as noted above, but does not explicitly disclose a system comprising an access control list update module configured to update the access control list according to the access prohibition list.

However, Wilson discloses an access control list update module configured to update the access control list according to the access prohibition list (*Wilson*: paragraph [0245], lines 13-16; *The examiner insists that the basic functionality of this limitation is simply updating a first list (access list) based on the changes made in a second list (prohibition list). This is obvious and well known in the art. The Wilson reference clearly shows updating a first list based on the changes made in a second list. So the examiner maintains that there is no distinct feature in the updating of a first list based on the changes in a second list to patentably distinguish the Wilson reference from the what the applicant is claiming here.*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Wilson noted above for the purpose of updating a first list based on the changes in a second list (*Wilson: paragraph [0245], lines 13-16*). The skilled artisan would have been motivated to improve the previously mentioned combination per the above in order to maintain data consistency between two changing lists.

5. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wilson and further in view of U.S. Patent Application Publication Number 2004/0153552 issued to Dirk Trossen et al. (hereinafter "Trossen").

**Claim 6:**

The combination of Ho, Kavalam, Wiik, and Wilson discloses all the elements of claim 5, as noted above, but does not explicitly disclose wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

However, it should be noted for the record though that Wiik does explicitly suggest providing access rights for only a certain predetermined period of time (*Wiik: column 2, lines 17-20 and column 3, lines 19-20; In the first reference note specifically "card validity time". And in the second reference note specifically the "start work time" and the "stop work time". These times represent times when the access to a certain access controller will start and stop respectively.*).

Furthermore, Trossen discloses wherein the list update module deletes the user information on the access prohibition list at a predetermined timing (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; In order to clarify the record, all that the applicant is claiming here is simply the changing of access rights at a predetermined period of time. By deleting the user information from the*

*prohibition list, the access rights of the user are no longer blocked. The user may have access again to all resources if added to appropriate access control lists, but that much is not stated here. The references cited from the Trossen reference clearly show a changing of access rights at a certain predetermined period of time. Further, in the second reference cited above, Trossen shows deleting this the users information from the database when the subscription ends. When the subscription ends, the user no longer has access to the resources granted by the subscription. This subscription ends at a predetermined period of time. The examiner maintains that the Trossen reference and invention claimed by the applicant in claim 6 are performing exactly the same function, and therefore the two inventions are not patentably distinct, because they both perform the same operation, in essentially the same manner, of canceling access rights at a predetermined period of time.).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Trossen noted above for the purpose of including an expiration time for access rights (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14*). The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that upon reaching a certain predetermined time, a status change notification message could be displayed showing the change in access rights of a user (*Trossen: paragraph [0002], lines 14-17; The examiner would like to bring to the applicant's attention that the reason or motivation to modify the reference may often suggest what the inventor has done, but for a different purpose or to solve a different problem. It is not necessary that the prior art suggest the combination to achieve the same advantage or result discovered by the applicant (In re Linter, 173 USPQ 560 (CCPA 1972) and In re Dillon, 16 USPQ2d 1897 (Fed. Cir. 1990)).*).

**Claim 7:**

The combination of Ho, Kavalam, Wiik, Wilson, and Trossen discloses all the elements of claim 6, as noted above, and Trossen further discloses wherein the predetermined timing is

Art Unit: 2163

after the update of the access control list has been completed (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time.*

*This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).*

**Claim 8:**

The combination of Ho, Kavalam, Wiik, Wilson, and Trossen discloses all the elements of claim 6, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.).*

6. Claims 9-10, 18, 20, 23, and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik and further in view of U.S. Patent Application Publication Number 2004/0203589 issued to Jiwei R. Wang et al. (hereinafter "Wang").

**Claims 9, 18, 20, 23, 27, and 28:**

The combination of Ho, Kavalam, Wiik and Wang discloses an access controller that controls an access to an information resource stored in a storage device connected to the access controller via a network, a plurality of the access controllers and storage devices being connected via the network, each of the access controllers having an access control list on which access right

Art Unit: 2163

to each information resource stored in the storage devices is recorded, and each of the access controllers having an access prohibition list on which access prohibited users are recorded who are prohibited from accessing any information resource stored in the storage devices,

and Ho explicitly discloses the access controller comprising:

an access restriction module (*Ho: paragraph [0004], lines 1-9 and paragraph [0009], lines 7-9 and paragraph [0010], lines 7-9; The content management system is the access restriction module.*) configured to restrict access to each information resource stored in a storage device and listed on the access control list of the access controller on which access right to each information resource is recorded (*Ho: paragraph [0003], lines 2-9 and paragraphs [0028]-[0031] and paragraph [0078], lines 6-10; Note specifically in the first reference cited "storage of an access control list (ACL) for each data entity to which access is to be controlled." Paragraph [0001], lines 9-11 defines a data entity.*).

Ho does not explicitly disclose:

a receiving module configured to receive user information of an access prohibited user, from one of the other access controllers connected to the network;

a list update module configured to update the access prohibition list of the access controller, which records user information of access to prohibited users, according to the received user information.

Kavalam also discloses an access control module to control access to network resources with the use of access control lists (*Kavalam: Fig. 1, 116 and paragraph [0062], lines 5-8*). Examiner notes that Kavalam does not explicitly disclose the use of an access prohibition list (or black-list) to intercept or restrict user access, but Kavalam does explicitly suggest protecting system resources by such strategies "lock down", isolation, and sandboxing of users or systems when

Art Unit: 2163

either accidental or malicious actions occur that could harm system resources (*Kavalam: paragraph [23], lines 23-28*). In order to “lock down”, isolate, or sandbox a particular user or system, a system administrator would have to have some means to detect that an accidental or malicious act either has already occurred, is currently occurring, or may occur in the future.

In order to satisfy the suggestion of combining additional methods of protecting system resources with the use of an access control module using access control lists, examiner asserts that it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ho, as suggested by Kavalam with the teachings of Wiik noted below.

Wiik discloses:

a receiving module configured to receive user information of an access prohibited user, from one of the other access controllers connected to the network (*Wiik: column 5, lines 9-11; Note that the black list stored in the RAM of the locking mechanism can receive updates to the black-list in the form of user ID's being added to the black-list. Since it can receive updates in the form of user ID's, it must have a receiving module to receive user information.*);

an access interception module configured to intercept the access by an access prohibited user listed on an access prohibition listed on an access prohibition list on an access prohibition list of the access controller (*Wiik: column 5, lines 7-9; The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to*

*add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.);*

a list update module configured to update the access prohibition list of the access controller, which records user information of access to prohibited users, according to the received user information (Wiik: column 5, lines 9-11; *The black-list is updated by the lock communicator (admin access controller) according to user ID's.*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a black-list, or prohibited user list, as part of an access controller (Wiik: column 5, lines 7-11). The skilled artisan would have been motivated to improve the invention of Ho per the above such that upon making a decision to cancel a given individual's access rights, the individual could be added to a black-list resulting in the immediate loss of access to a given resource (Wiik: column 5, lines 7-11 and column 8, lines 11-14).

The combination of Ho, Kavalam, and Wiik disclose have so far disclosed all the elements of claim 9, as noted above, and Wiik further discloses an access interception module configured to restrict the access by reference to an access prohibited list (Wiik: column 5, lines 7-9; *The black-list is the access prohibited user list. The black-list is stored in the RAM of a locking mechanism (access interception module), which intercepts the access of a user listed on the black-list. Note that a user obtaining the key could have access and be on the way to unlock the locking mechanism (or access interception module). Then after the key is issued, the administrator could choose to add the user's name to the black-list. This immediately cancels the users action rights and effectively 'intercepts' the access of the user.*). None of the previously mentioned combination explicitly discloses referencing the access prohibition list **prior to** the access control list.

Art Unit: 2163

However, Wang explicitly discloses restricting access by first referencing a prohibited list **prior to** the access control list (*Wang: paragraph [0033], liens 1-3; The black-list is the prohibited list and the white-list is the access allowed list.*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the previously mentioned combination with the teachings of Wang noted above for the purpose of modifying the order in which the lists are accessed. The skilled artisan would have been motivated to further improve the previously mentioned combination per the above such that the system is capable of checking a black list of access rights prior to checking an access rights allowed list (*Wang: paragraph [0033], lines 1-3*).

**Claim 10:**

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 9, as noted above, and Wiik further discloses wherein the access interception module also intercepts an uncompleted access (*Wiik: column 8, lines 11-15; When the access is denied (by not unlocking the locking mechanism or access controller due to inclusion on a black-list), the access is interrupted and therefore not completed.*).

7. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wang and in further view of Wilson.

**Claim 11:**

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 9, as noted above, but does not explicitly disclose an access control list update module configured to update the access control list according to the access prohibition list.



However, Wilson discloses an access control list update module configured to update the access control list according to the access prohibition list (*Wilson: paragraph [0245], lines 13-16; The examiner insists that the basic functionality of this limitation is simply updating a first list (access list) based on the changes made in a second list (prohibition list). This is obvious and well known in the art. The Wilson reference clearly shows updating a first list based on the changes made in a second list. So the examiner maintains that there is no distinct feature in the updating of a first list based on the changes in a second list to patentably distinguish the Wilson reference from the what the applicant is claiming here.*).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Wilson noted above for the purpose of updating a first list based on the changes in a second list (*Wilson: paragraph [0245], lines 13-16*). The skilled artisan would have been motivated to improve the previously mentioned combination per the above in order to maintain data consistency between two changing lists.

8. Claims 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ho in view of Kavalam in view of Wiik in view of Wang and in further view of Trossen.

**Claim 12:**

The combination of Ho, Kavalam, Wiik, and Wang discloses all the elements of claim 11, as noted above, but does not explicitly disclose wherein the list update module deletes the user information on the access prohibition list at a predetermined timing.

Furthermore, Trossen discloses wherein the list update module deletes the user information on the access prohibition list at a predetermined timing (*Trossen: paragraph [0032], lines*

9-11 and paragraph [0043], lines 10-14; This claim is rejected under the same reasons set forth in claim 6. See the rejection of claim 6 for an explanation as to why this reference applies.).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the previously mentioned combination with the teachings of Trossen noted above for the purpose of including an expiration time for access rights (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14*). The skilled artisan would have been motivated to improve the previously mentioned combination per the above such that upon reaching a certain predetermined time, a status change notification message could be displayed showing the change in access rights of a user (*Trossen: paragraph [0002], lines 14-17*).

**Claim 13:**

The combination of Ho, Kavalam, Wiik, Wang, and Trossen discloses all the elements of claim 12, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of the access control list has been completed (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6. The changing or setting of the predetermined time is obvious and well known in the art and is simply a design choice. For further explanation of the cited references see the rejection of claim 6.*).

**Claim 14:**

The combination of Ho, Kavalam, Wiik, Wang, and Trossen discloses all the elements of claim 12, as noted above, and Trossen further discloses wherein the predetermined timing is after the update of all access control lists of the access controllers has been completed (*Trossen: paragraph [0032], lines 9-11 and paragraph [0043], lines 10-14; This claim also strictly deals with the changing of*

Art Unit: 2163

*access rights at a certain time. This claim is rejected using the same rationale set forth in the rejection of claim 6.*

*The changing or setting of the predetermined time is obvious and well known in the art and is simply a design*

*choice. For further explanation of the cited references see the rejection of claim 6.).*

*Response to Arguments*

**Applicant Argues:**

Moreover, Kavalam has a U.S. filing data that is later than that of the present invention, and thus must rely on its provisional application filing date to antedate the present application so as to be available as a reference. However, the provisional contains only general disclosure of identity-based access control, with some specific examples, but without the disclosure of the passage relied on in the rejection (paragraph [0062] of the PGP).

**Examiner Responds:**

Examiner is not persuaded. Fig. 10 submitted with the provisional application clearly supports paragraph [0062] of the PGP issued to Kavalam. Note specifically the using Access Control Lists (ACL) in conjunction with read-only files. This is direct support for paragraph [0062], lines 5-8. The rejections under 35 U.S.C. 103(a) are upheld.

**Applicant Argues:**

Respectfully, the system settings that Kavalam seeks to protect from change, while denoted "system resources" in the patent, are operating system resources, not information resources such as data files, images, music, etc. as required by the claims. Moreover, although Kavalam protects against change to the system settings, it is not "user access" that is prevented in the sense of the claimed invention. Indeed, it is not the same "user access" as even disclosed by Ho, which is an argument against the motivation to combine with Ho.

Further, despite that Ho, Kavalam, and Wiik disclose such disparate technologies that their combination is dubious, any possibly motivated combination would still fail to include at least the claimed access control module and list update module as advanced above, and would be limited to restricting physical access to the system settings of a single computer.

**Examiner Responds:**

Examiner is not persuaded. With respect to the combination of references, all of the references clearly deal with access control. Since they are all directed to the solving the same problem, their combination is hardly 'dubious'.

Art Unit: 2163

Examiner also notes that all limitations of the Applicant's claims are clearly set forth in the rejections given above. Furthermore, the Examiner is confident that there is strong suggestion and motivation to combine the references. Therefore, the rejections given under 35 U.S.C. 103(a) are upheld.

**Applicant Argues:**

Wiik is cited against the claimed access control interception module, but actually discloses an electronic lock for restricting entry to a building, not for prohibiting access to an information resource as claimed. Wiik is also cited against the claimed list update module, but Wiik only discloses updating of a single physical lock, whereas the claimed list update module must be configured to update each of the access prohibition lists of each of the claimed plurality of access controllers on the network.

**Examiner Responds:**

Examiner is not persuaded. Column 5, lines 7-11 clearly discloses an interception module. Note specifically, "A black list in RAM, with a capacity of 20 user ID codes, can be used to immediately cancel individual cards in a lock." The immediate cancellation of access rights is clearly implemented by an 'interception module'.

Further note Column 5, lines 9-11. Note that each black-list is updated by the lock communicator (admin access controller). The update to the black list is received at the access controller (locking mechanism). This occurs for each lock. So each list at each lock is updated.

The Wiik reference clearly teaches a method of access control using black lists or prohibited user lists in order perform access interception. The Ho reference clearly teaches access control to information resources using access control lists. And the Kavalam reference clearly suggests a lockdown or interception method when malicious activity is suspected to occur. Therefore, the Examiner believes it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the references of Ho, Kavalam, and Wiik in order to provide an access control module based upon access control lists, prohibitive user lists, and the interception of access as claimed by the Applicant.

For further explanation or clarification, see Examiner's above Office Action. The rejections given under 35 U.S.C 103(a) are upheld.

**Examiner Remarks:**

All other arguments set forth by the Applicant have been clearly and specifically addressed in prior Office Actions. The Examiner maintains the positions set forth in previous Office Actions.

***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

***Relevant Art***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is listed below.

- U.S. Patent Application Publication Number 2004/0044529
  - paragraph [0016] – checks to see if there is a registered “problem” with a user trying to log onto a computer system.

Art Unit: 2163

- paragraph [0022] – discloses using a blacklist to restrict or reject access of a user.
- U.S. Patent Application Publication Number 2005/0110609
  - paragraph [0020] – discloses using a ‘lockout list’ to detect an unauthorized user or device.
  - paragraph [0055] – discloses preventing a user from making an otherwise authorized access by identifying a user of a ‘lock out’ list.
- U.S. Patent Number 6,523,117
  - Column 7, lines 27-35 – discloses detecting if a user was entered on a black-list.
- U.S. Patent Number 7,007,093
  - Column 1, lines 18-19 – discloses wherein resource access is restricted by defining access control lists for each network resource.

### ***Contact Information***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrick A. Darno whose telephone number is (571) 272-0788.

The examiner can normally be reached on Monday - Friday, 9:00 am - 5:30 pm.

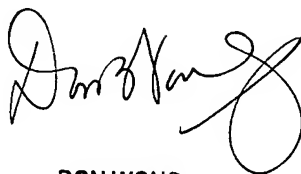
If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Don Wong can be reached on (571) 272-1834. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2163

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PD



DON WONG  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Patrick A. Darno  
Examiner  
Art Unit 2163

